

Fig. 1

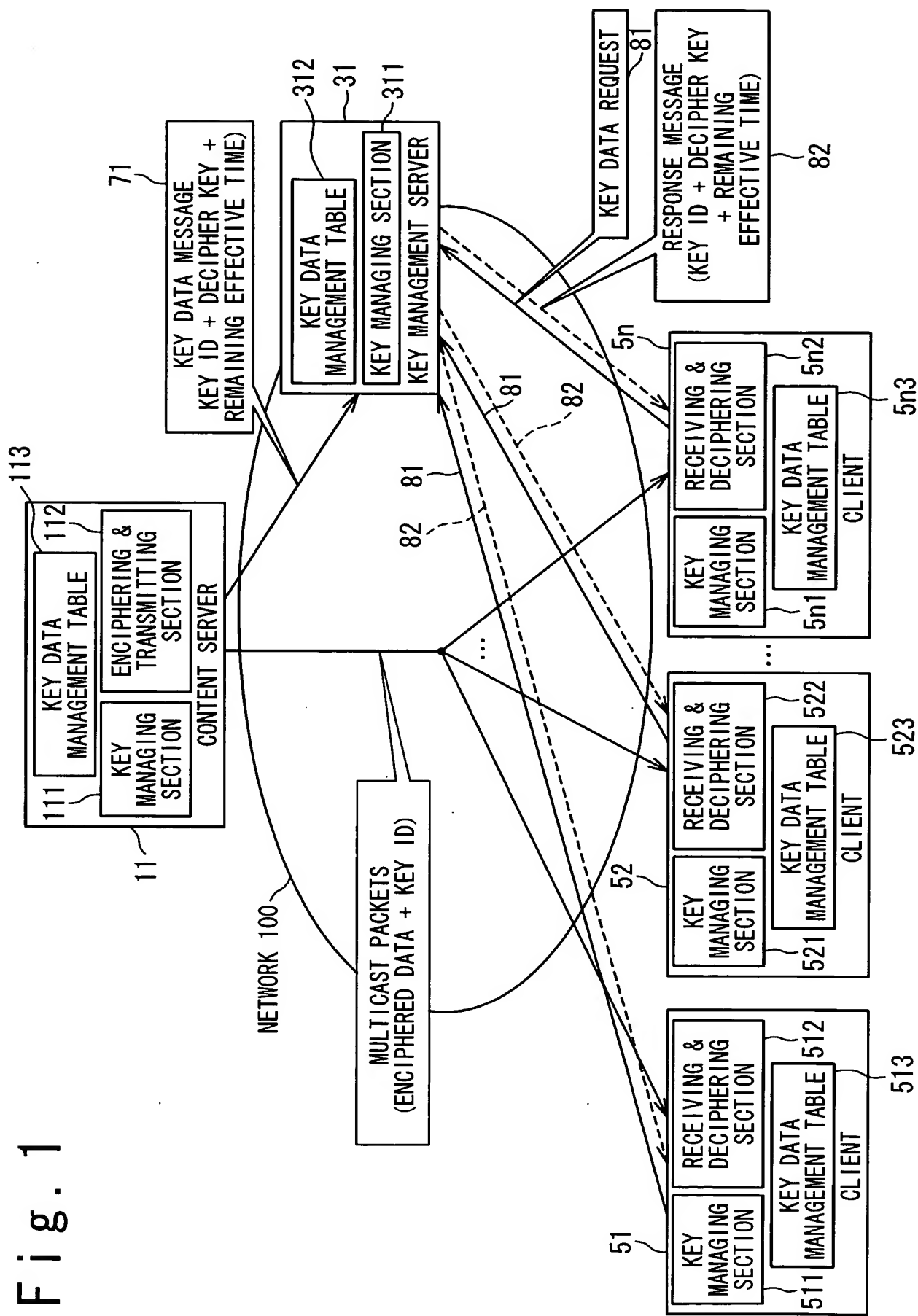


Fig. 2

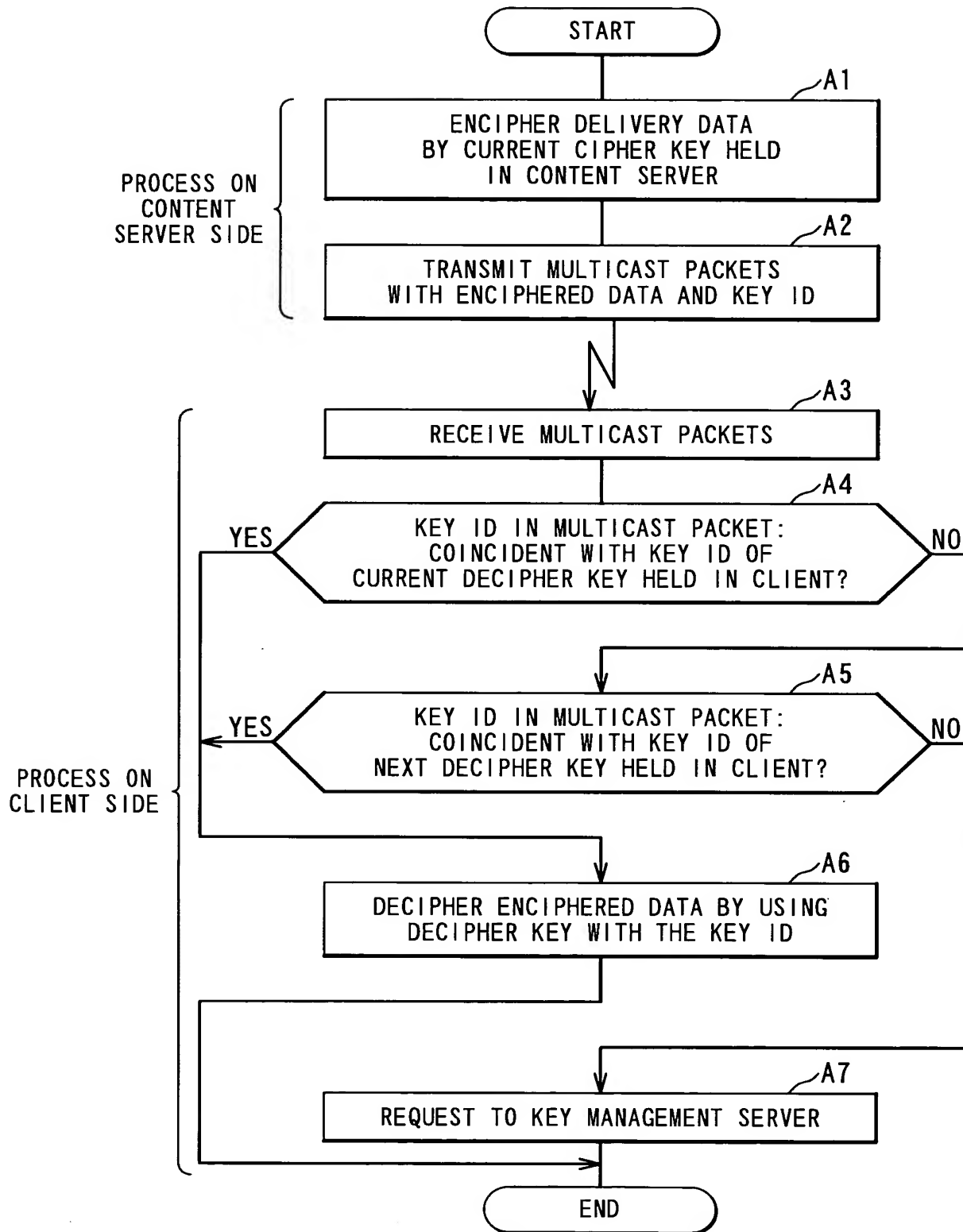


Fig. 3

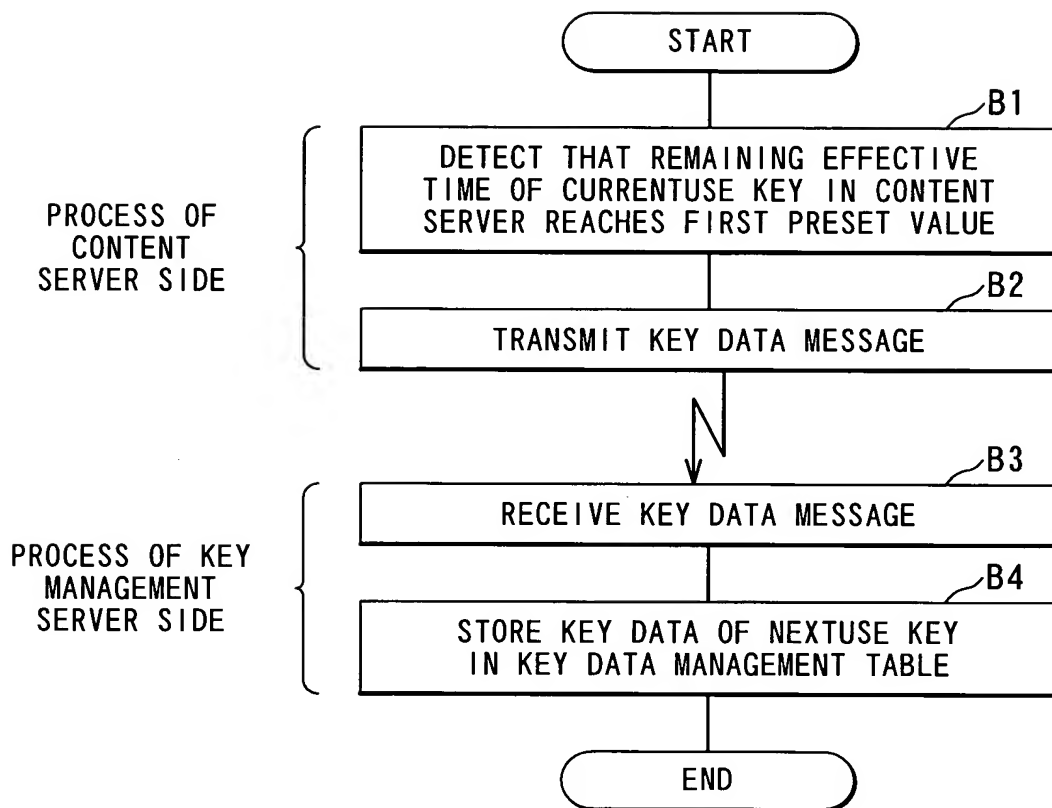
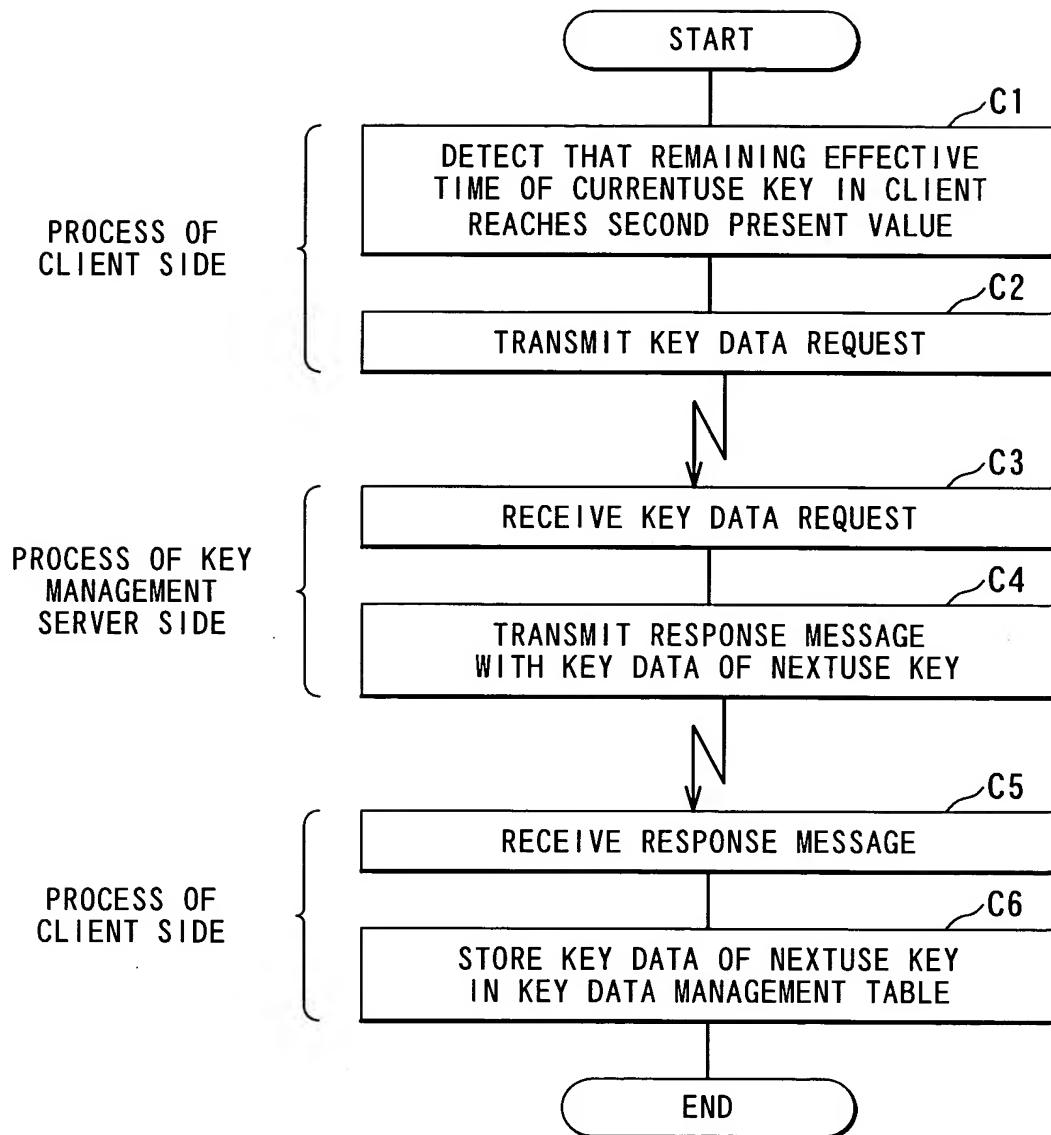


Fig. 4



# Fig. 5

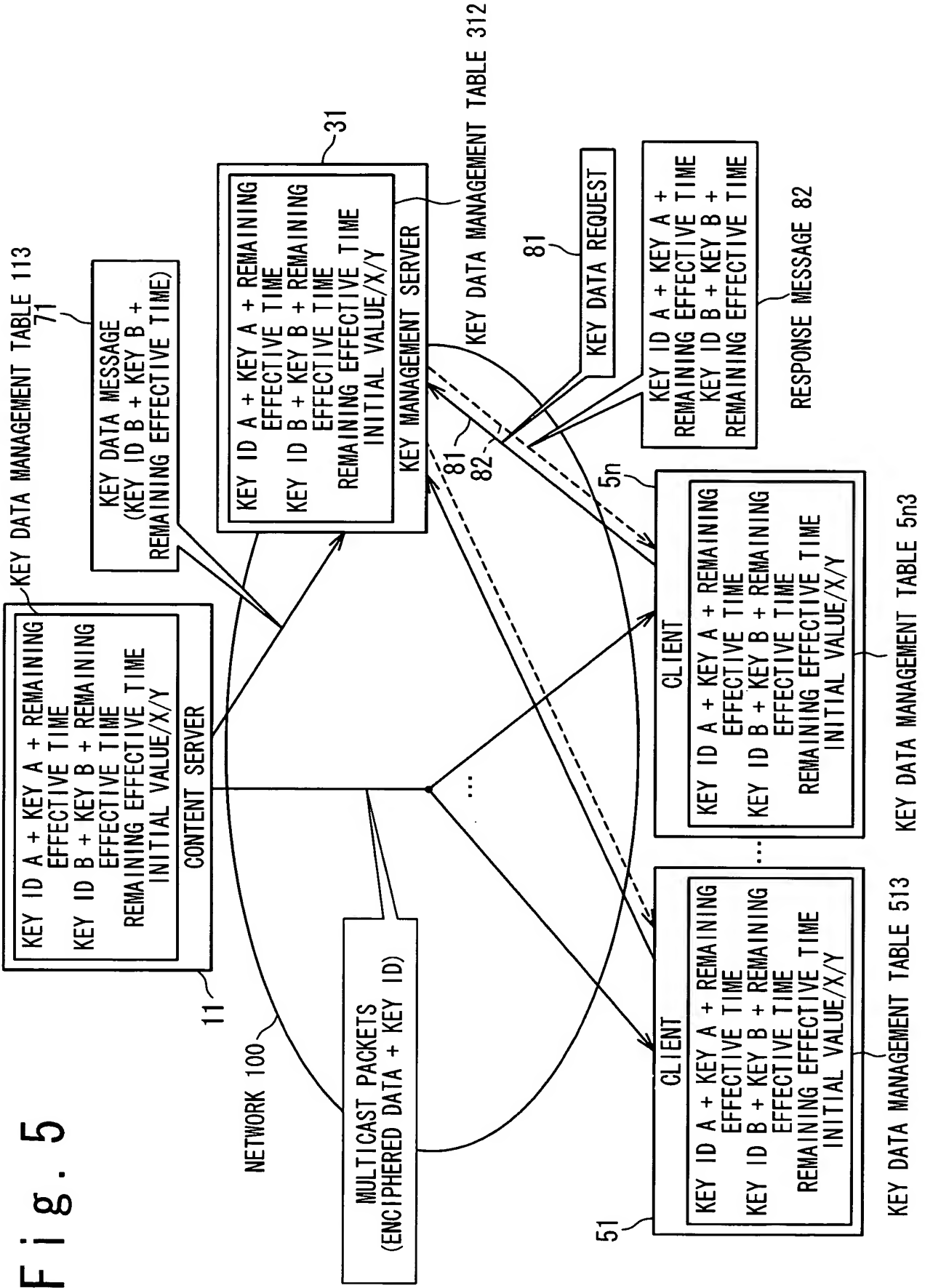


Fig. 6

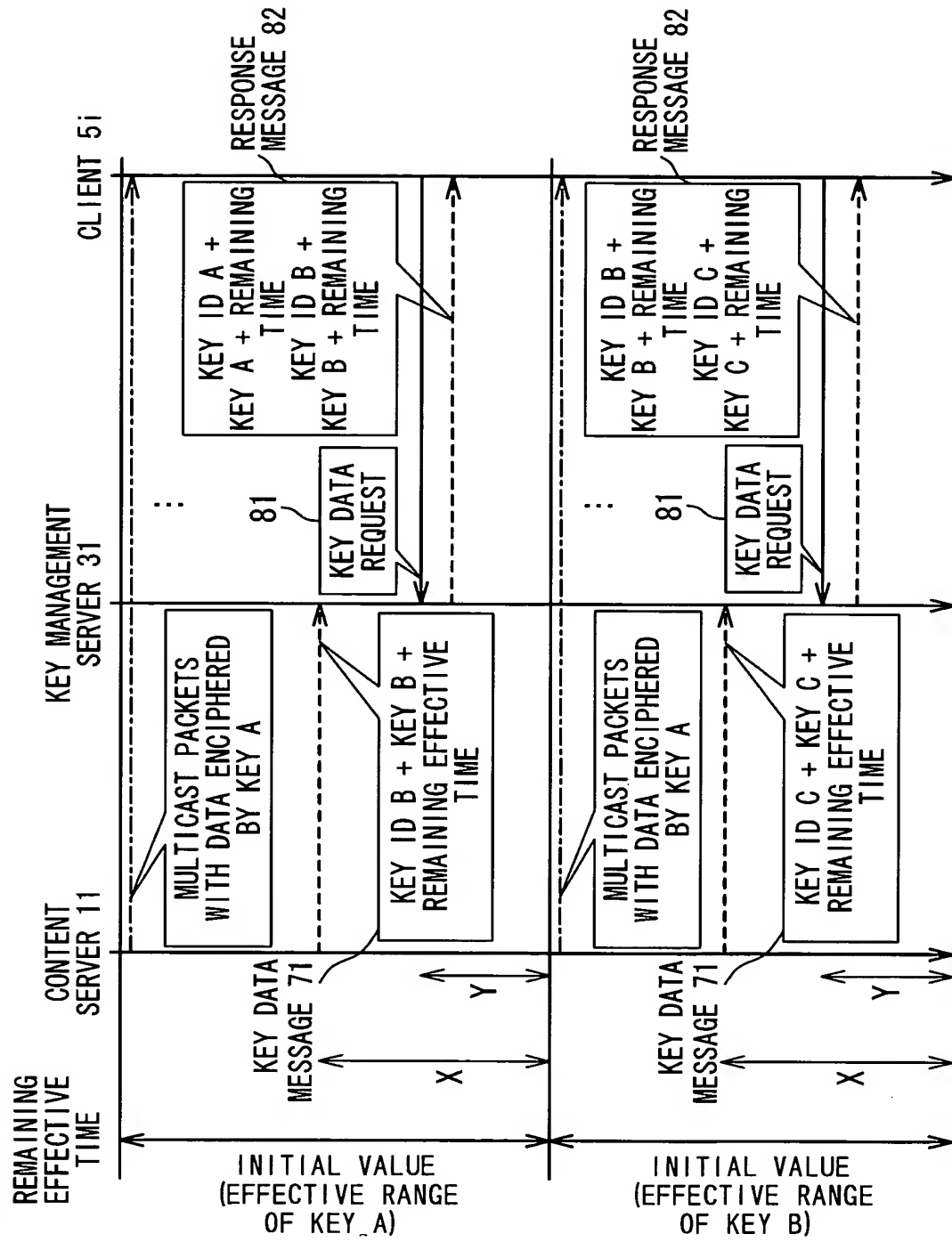


Fig. 7

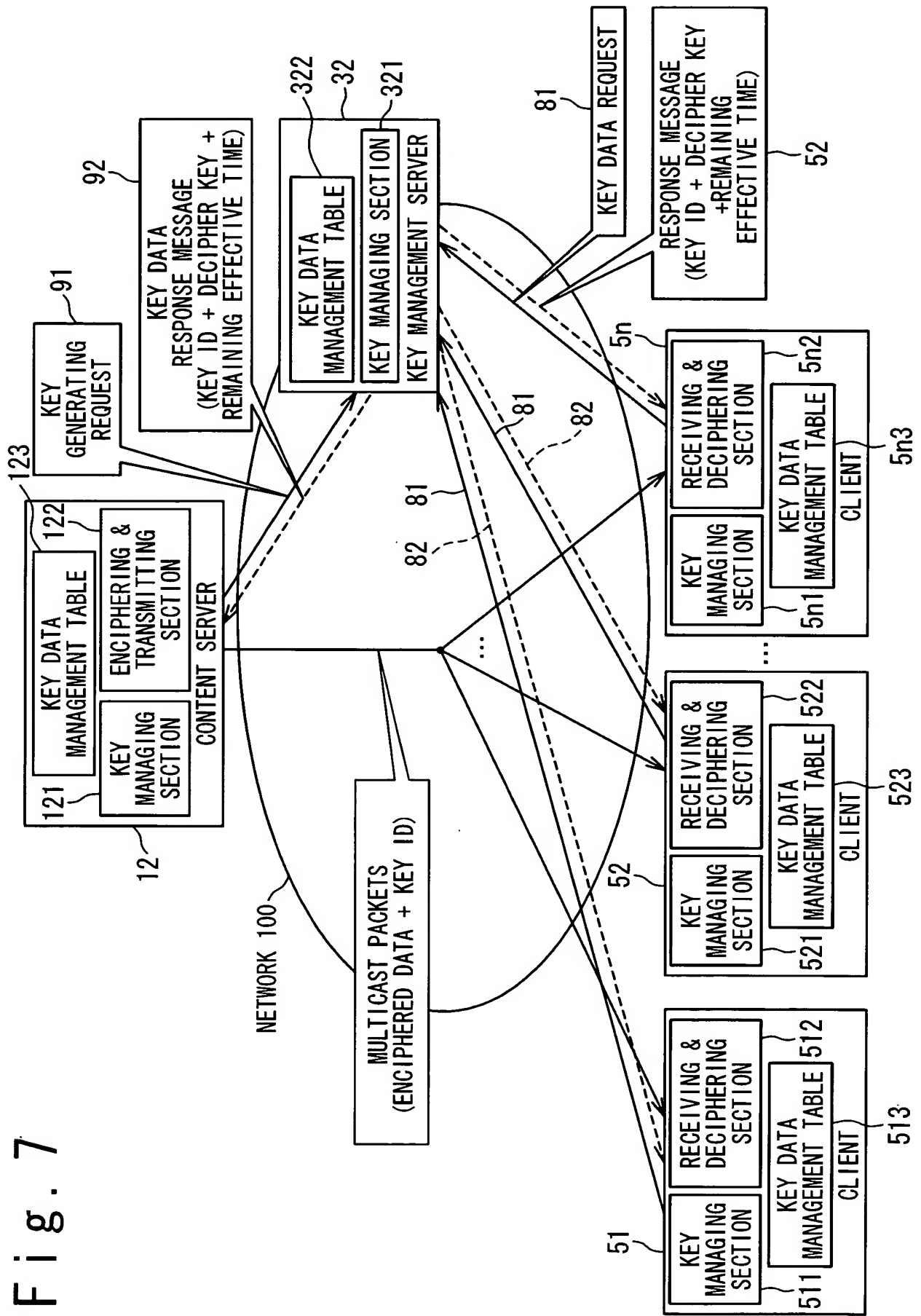


Fig. 8

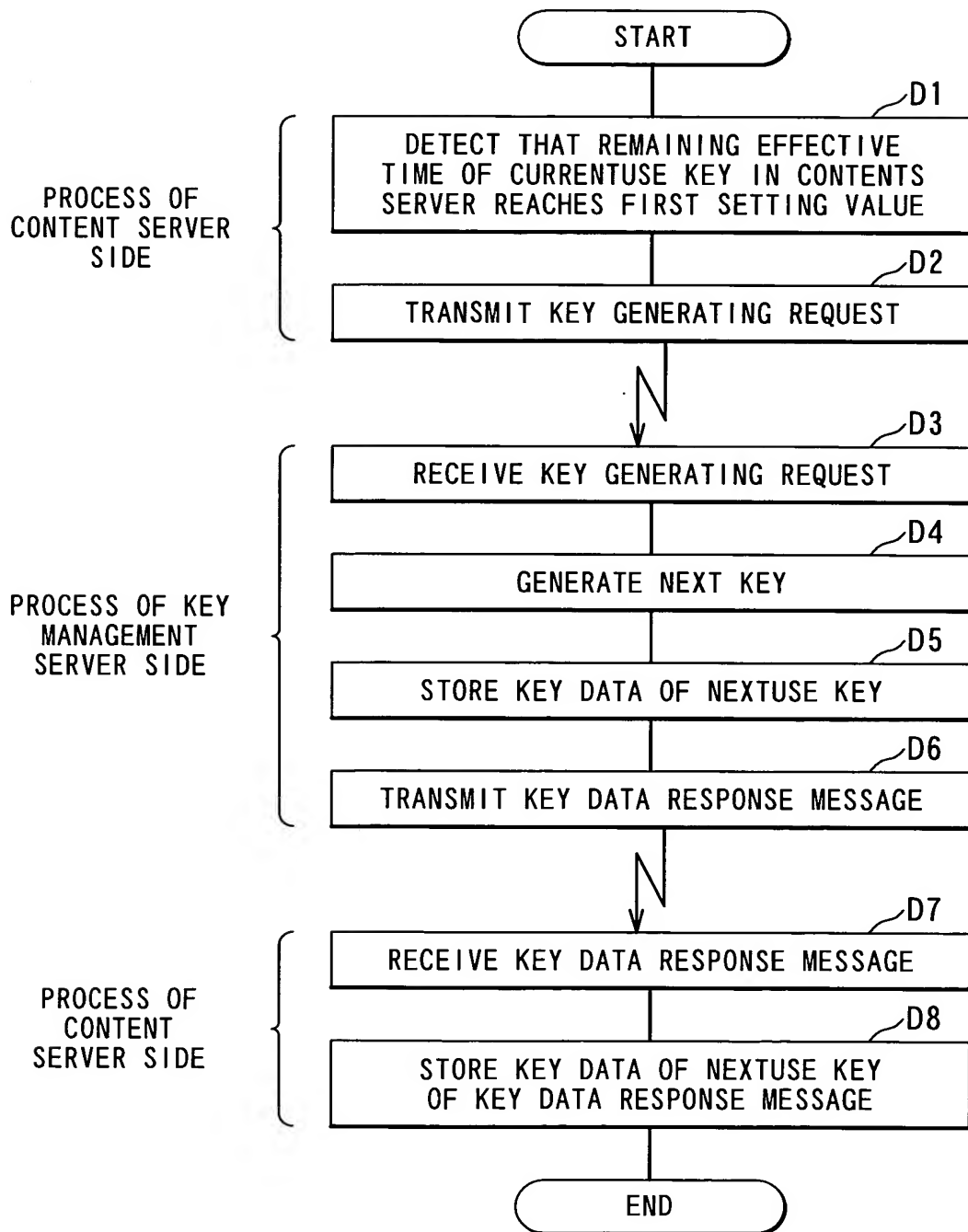




Fig. 9 is a block diagram illustrating a system for key replacement, involving a Content Server, a Key Management Server, and multiple Clients.

**Content Server (11):** Contains a Key Managing Section (111) and an Enciphering & Transmitting Section (112). It is connected to the Key Management Server (902) via a Network 100.

**Key Management Server (902):** Contains a Key Data Management Table (312) and a Key Managing Section (311). It receives a Key Data Message (71) from the Content Server (11) and sends a Key Replace Control Program for Key Management Server (82) and a Key Data Request (81) to the Clients (51, 52, 53, ..., 5n3).

**Clients (51, 52, 53, ..., 5n3):** Each client contains a Key Managing Section (511, 521, 531, ..., 5n1) and a Receiving & Deciphering Section (512, 522, 532, ..., 5n2). They receive Multicast Packets (Enciphered Data + Key ID) from the Content Server (11) and send a Key Data Request (81) to the Key Management Server (902). The Key Management Server (902) sends a Key Replace Control Program for Client (903) to the Clients.

**Network 100:** Facilitates communication between the Content Server (11) and the Key Management Server (902).

**Key Data Message (71):** Sent from the Content Server (11) to the Key Management Server (902).

**Key Replace Control Program for Key Management Server (82):** Sent from the Key Management Server (902) to the Clients.

**Key Data Request (81):** Sent from the Clients to the Key Management Server (902).

**Response Message (Key ID + Decipher Key + Remaining Effective Time):** Sent from the Clients to the Key Management Server (902).

**Key Replace Control Program for Client (903):** Sent from the Key Management Server (902) to the Clients.

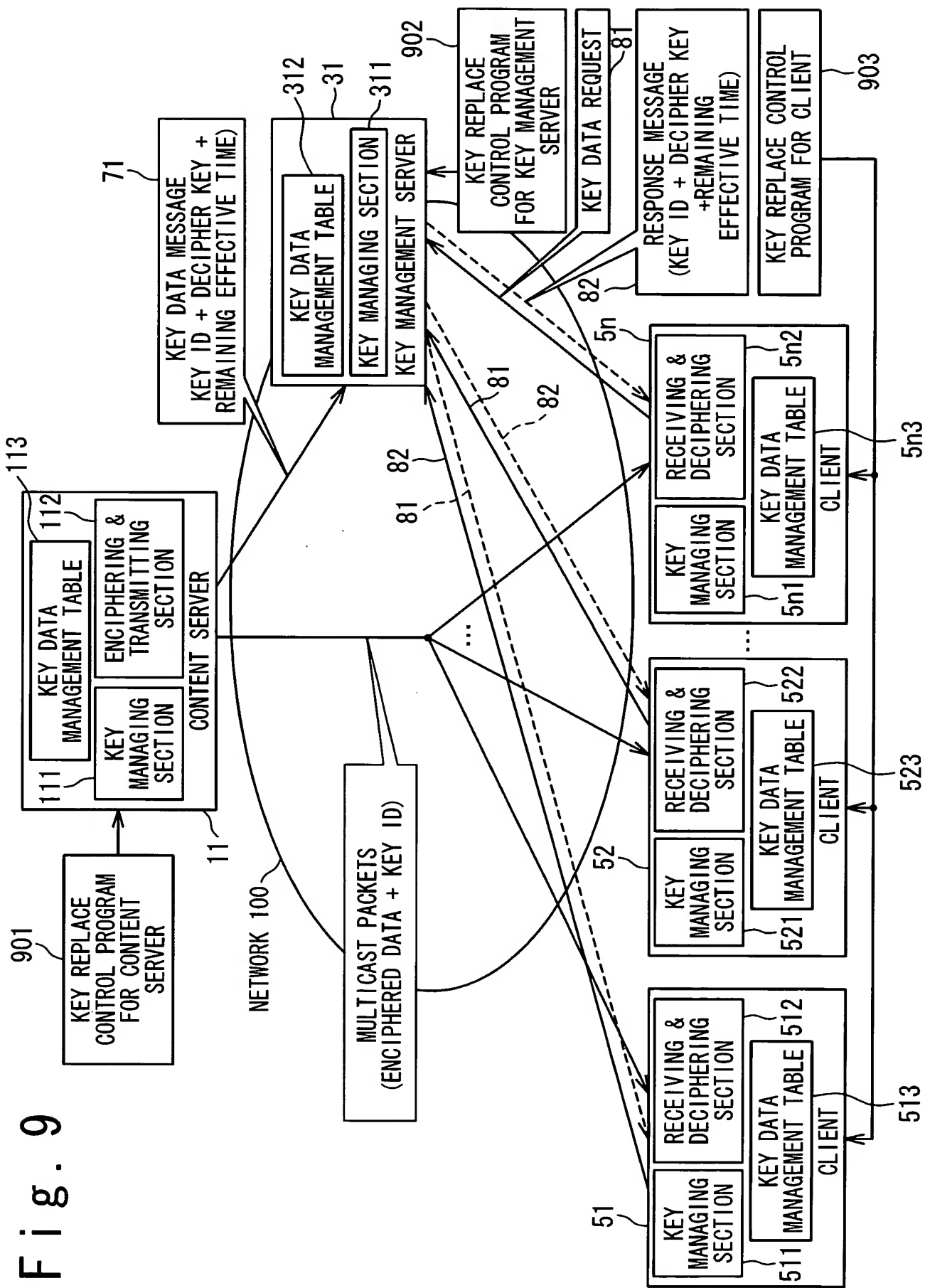


Fig. 10

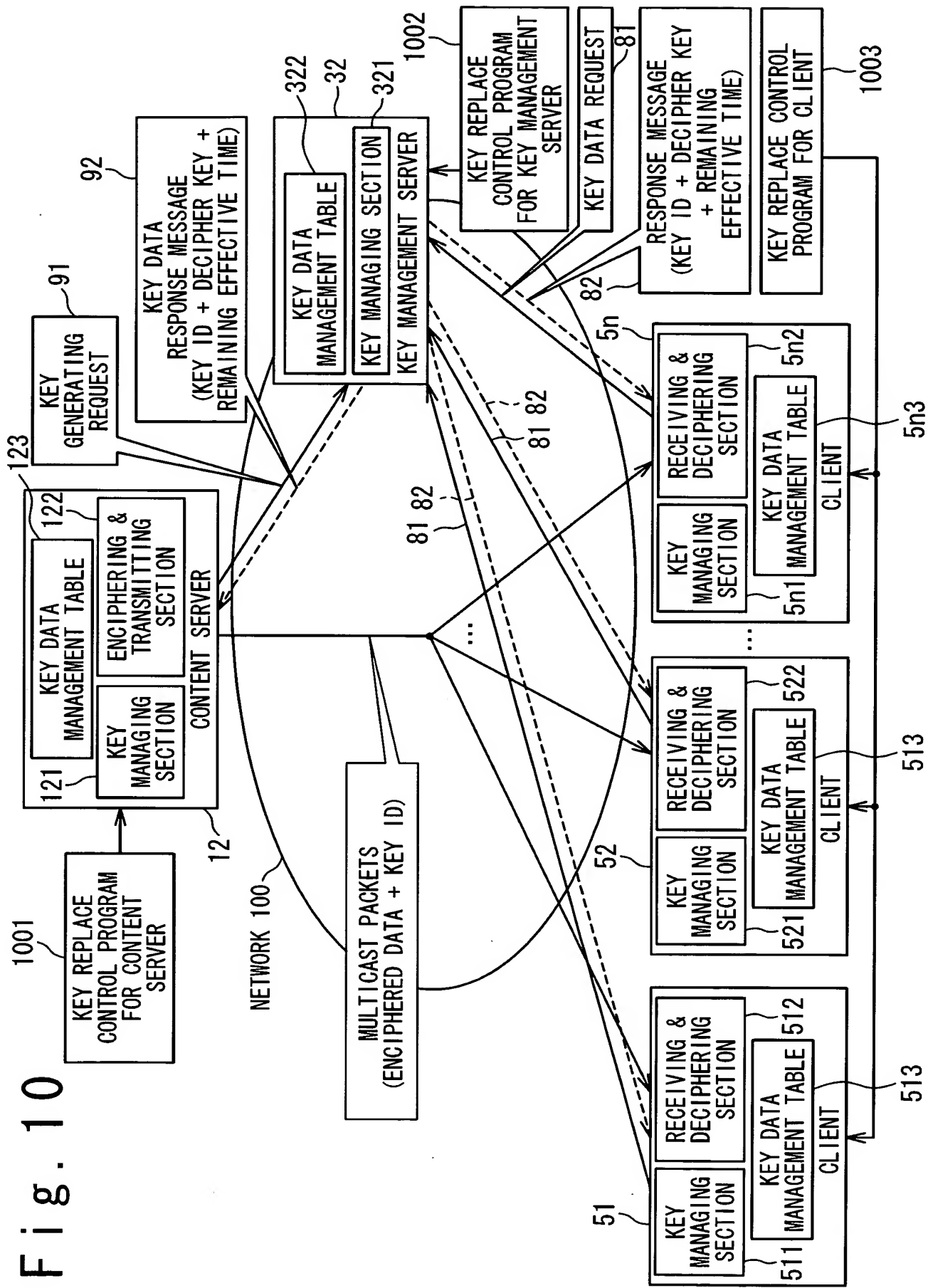
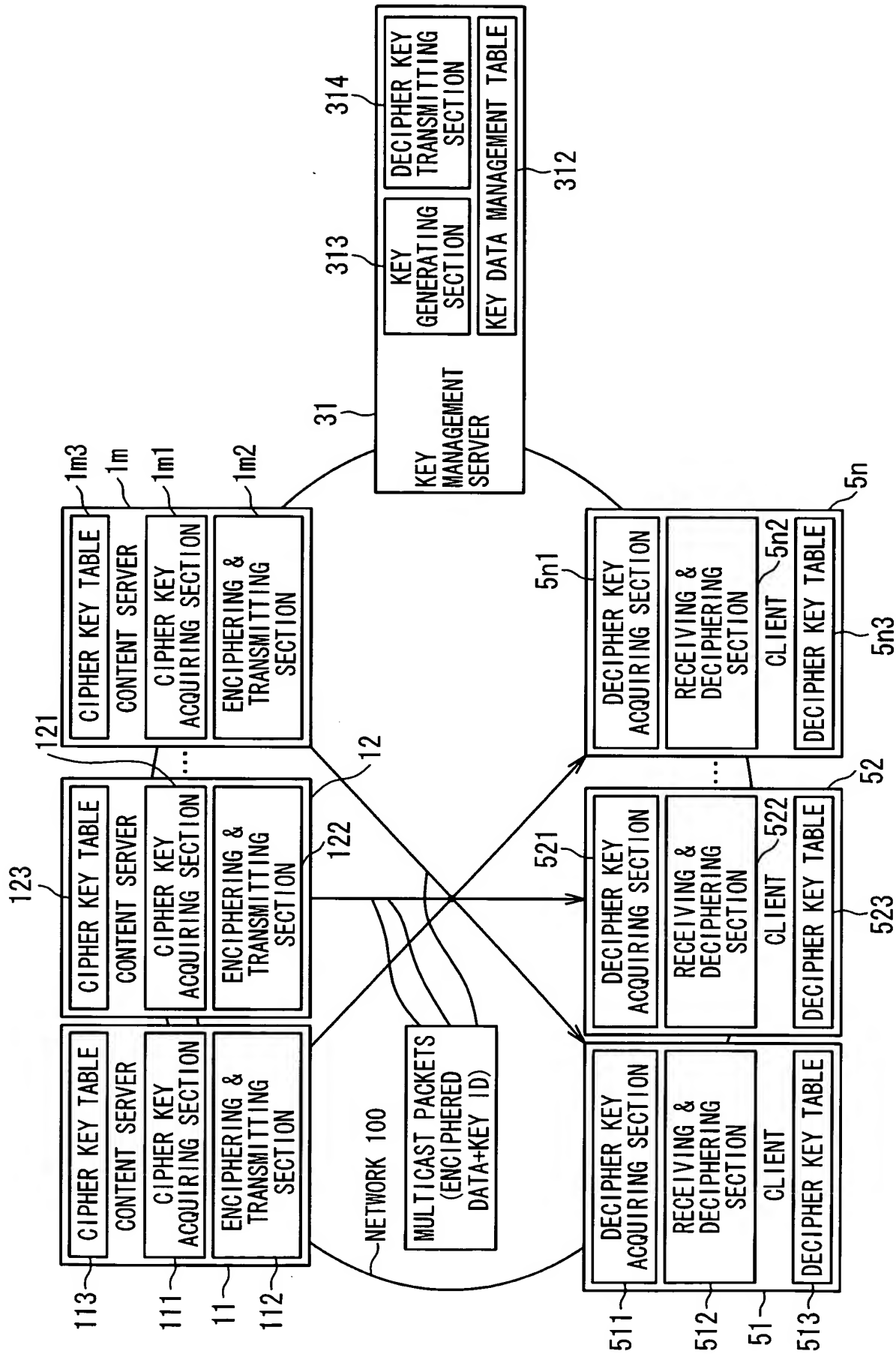


Fig. 11



# Fig. 12

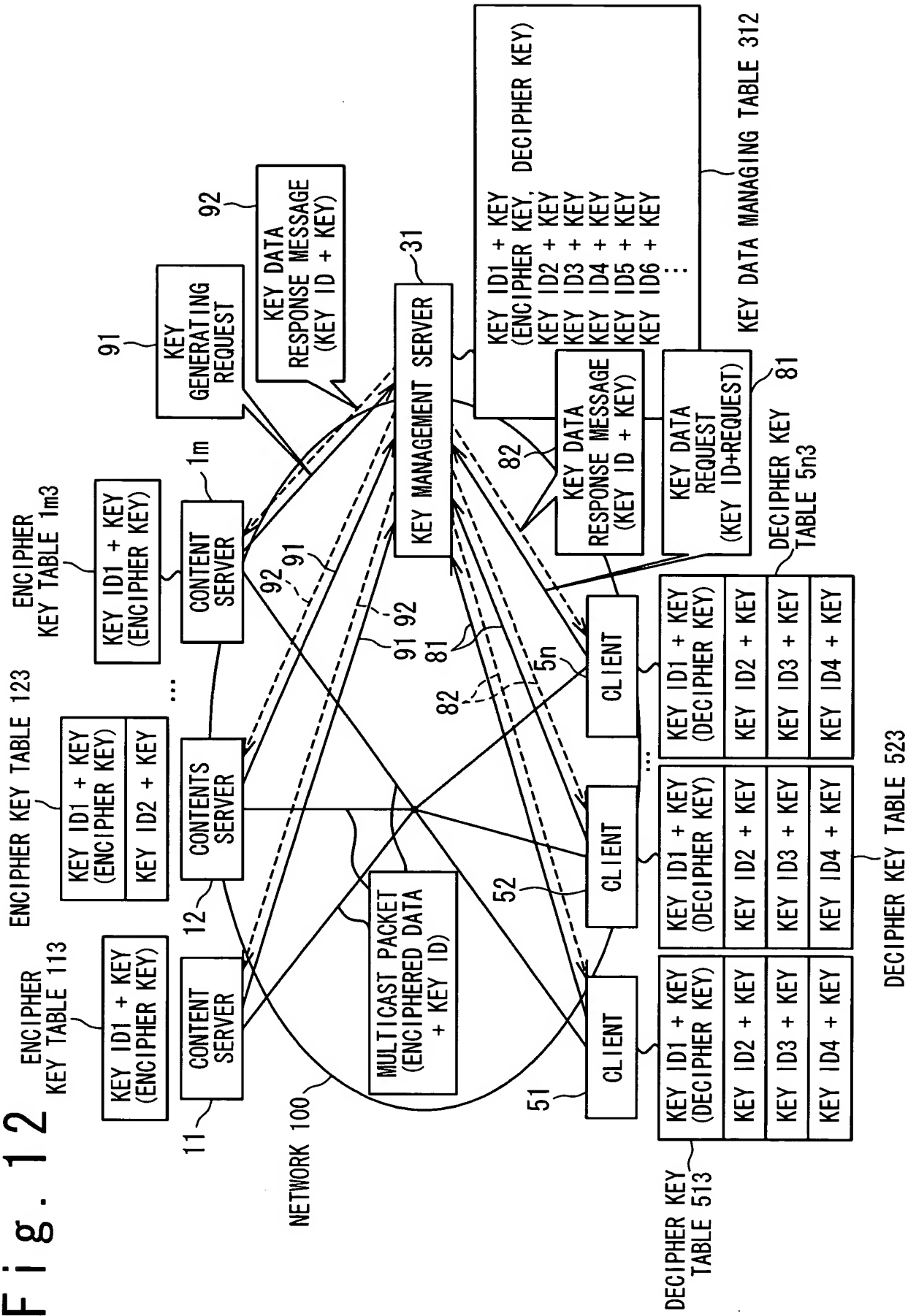


Fig. 13

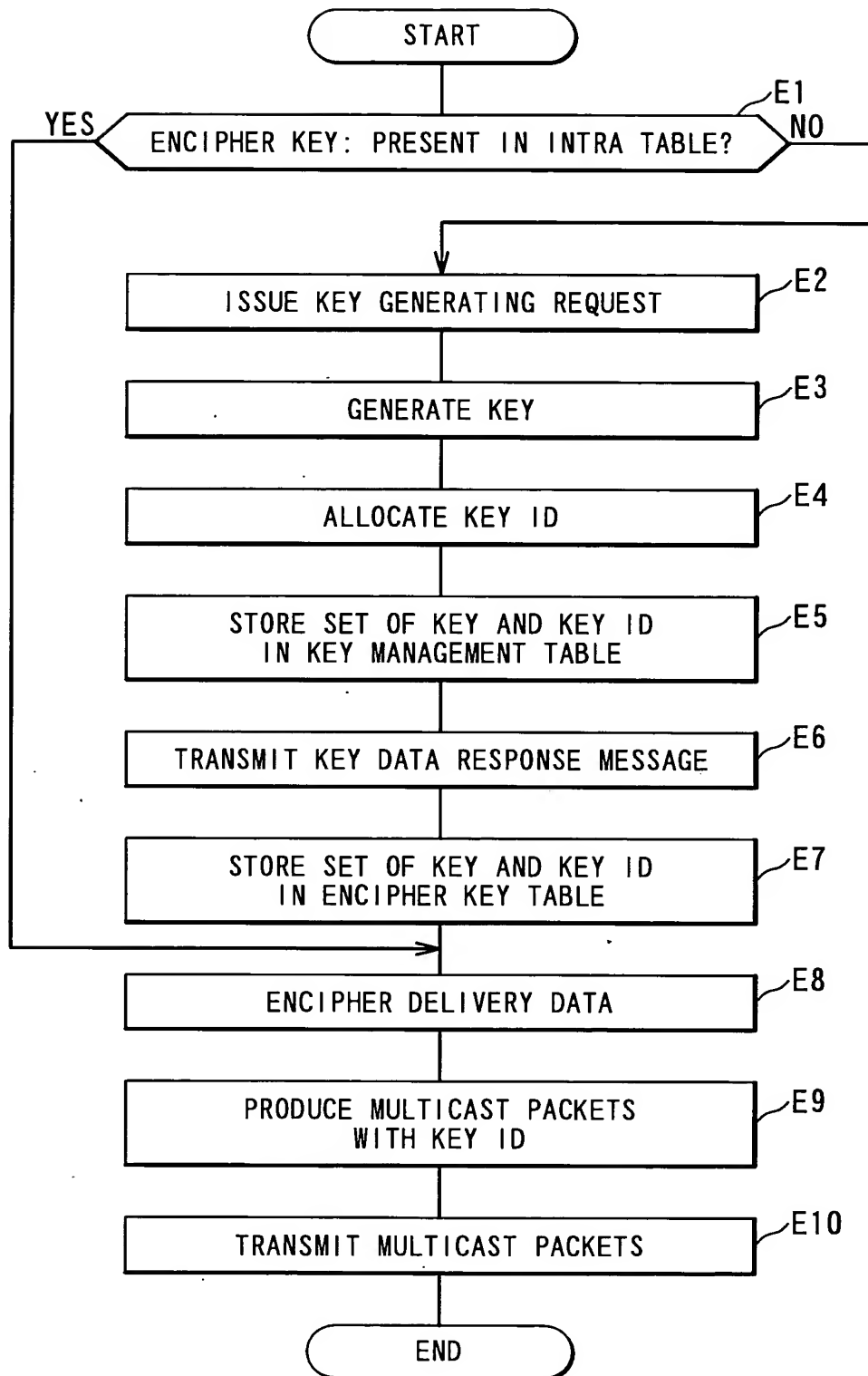


Fig. 14

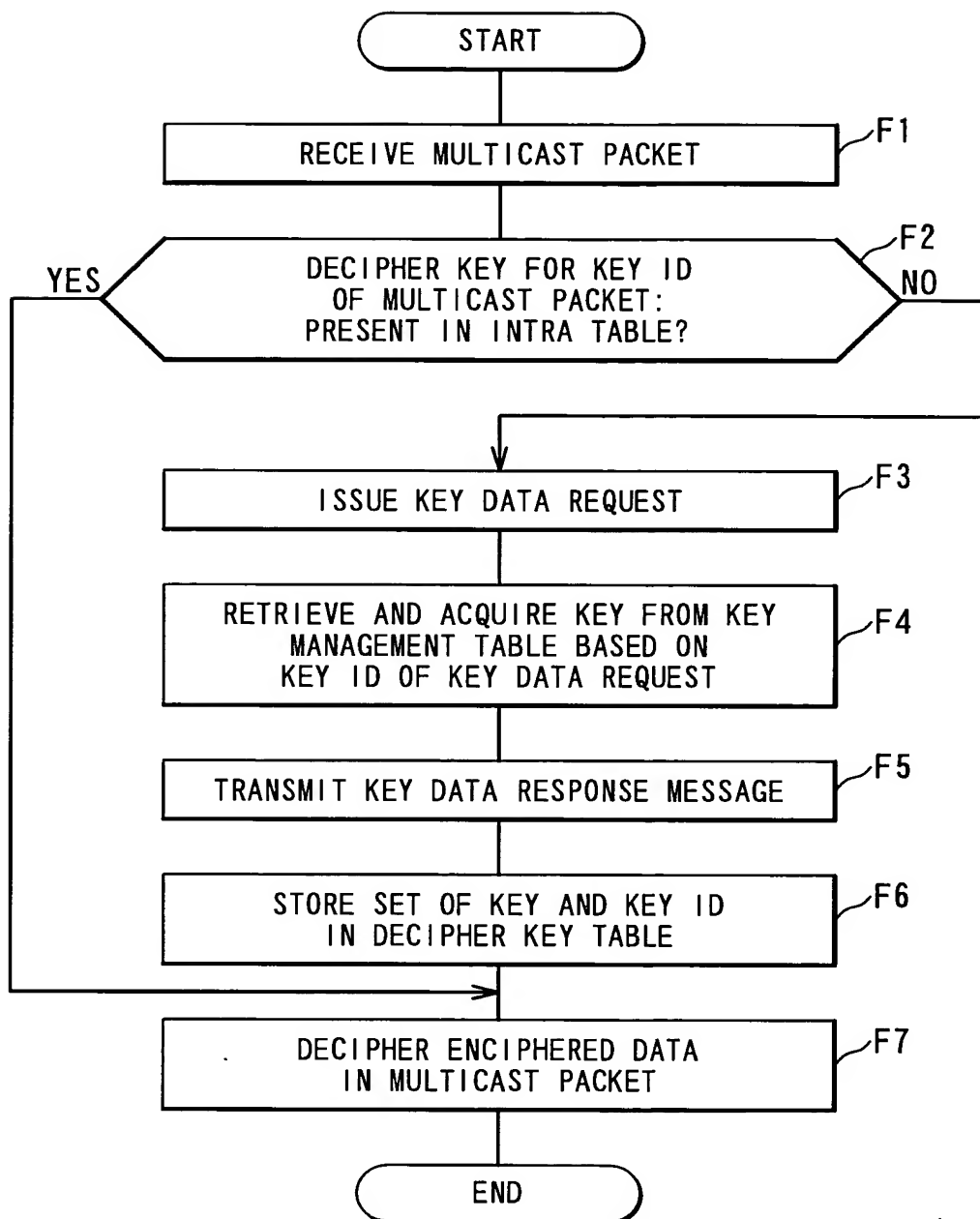


Fig. 15

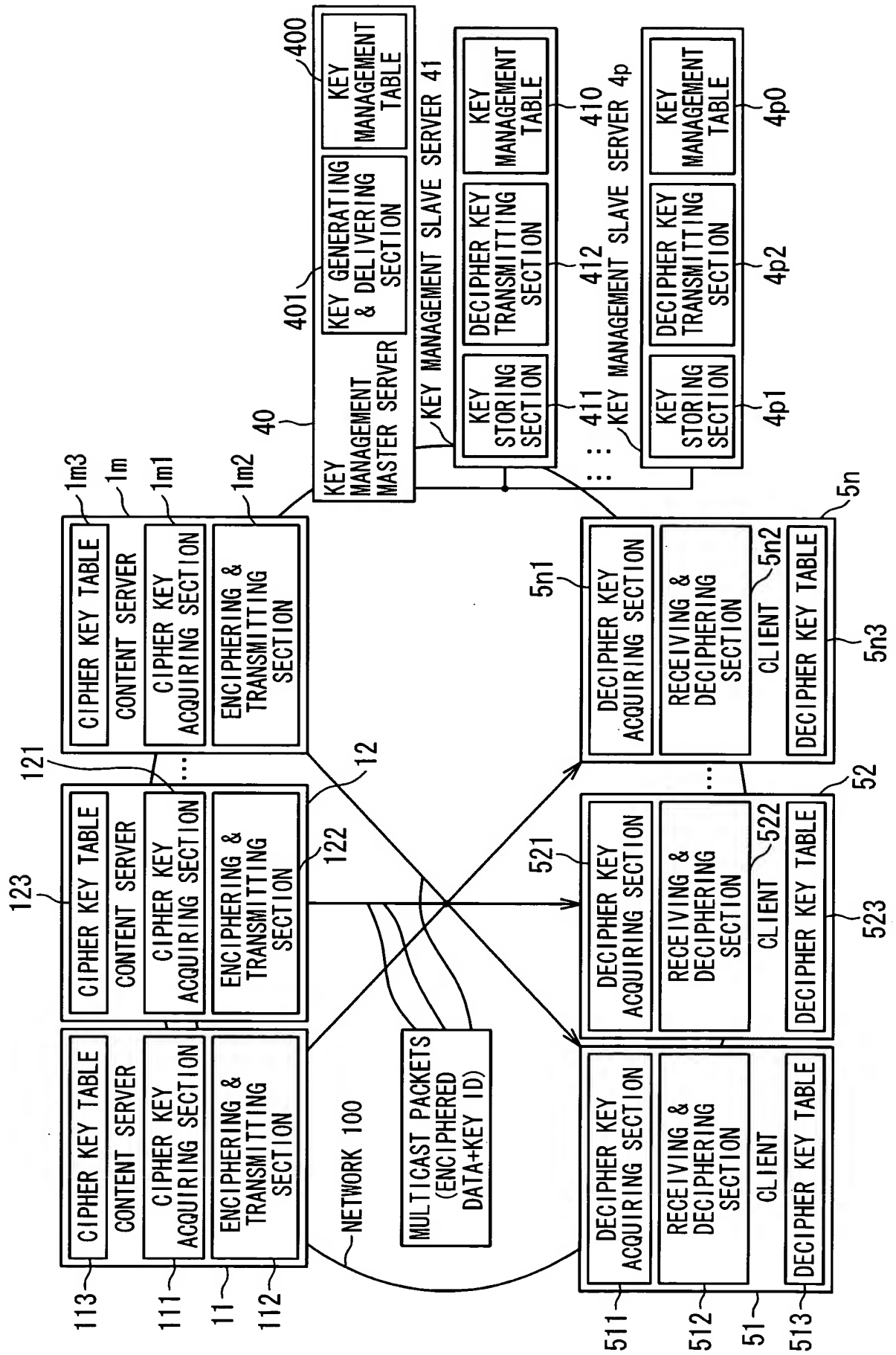


Exhibit 16

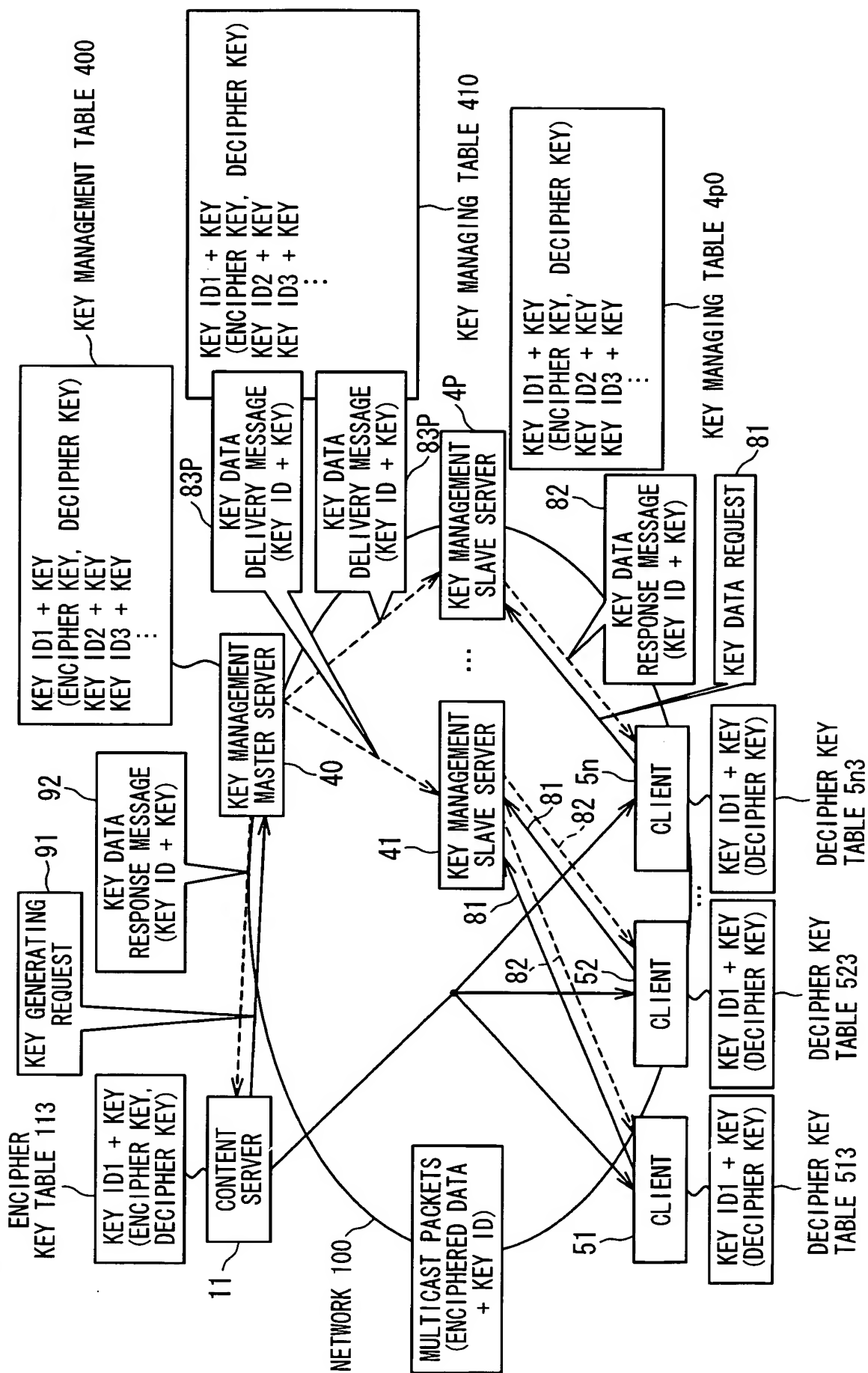




Fig. 17

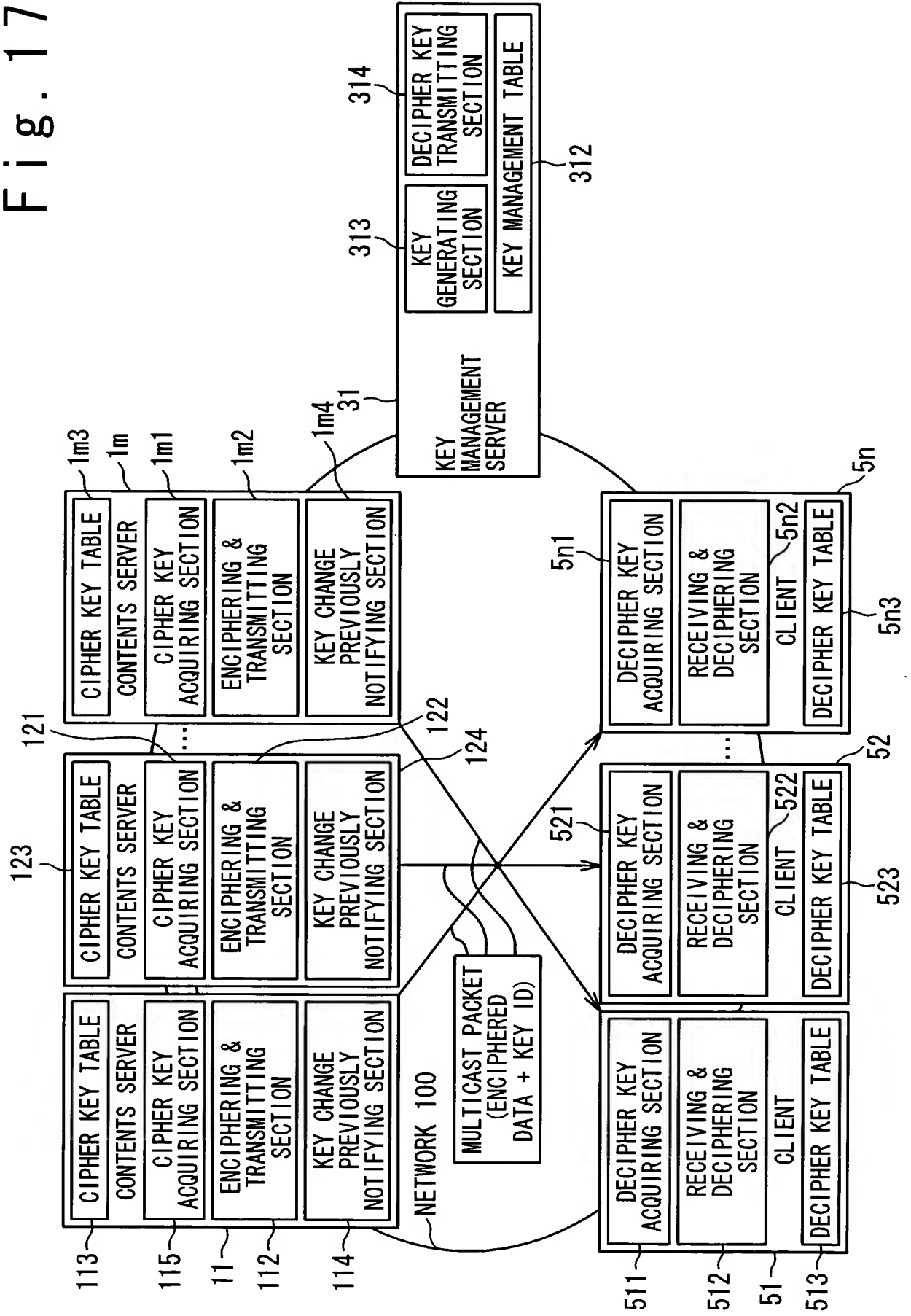


Fig. 18

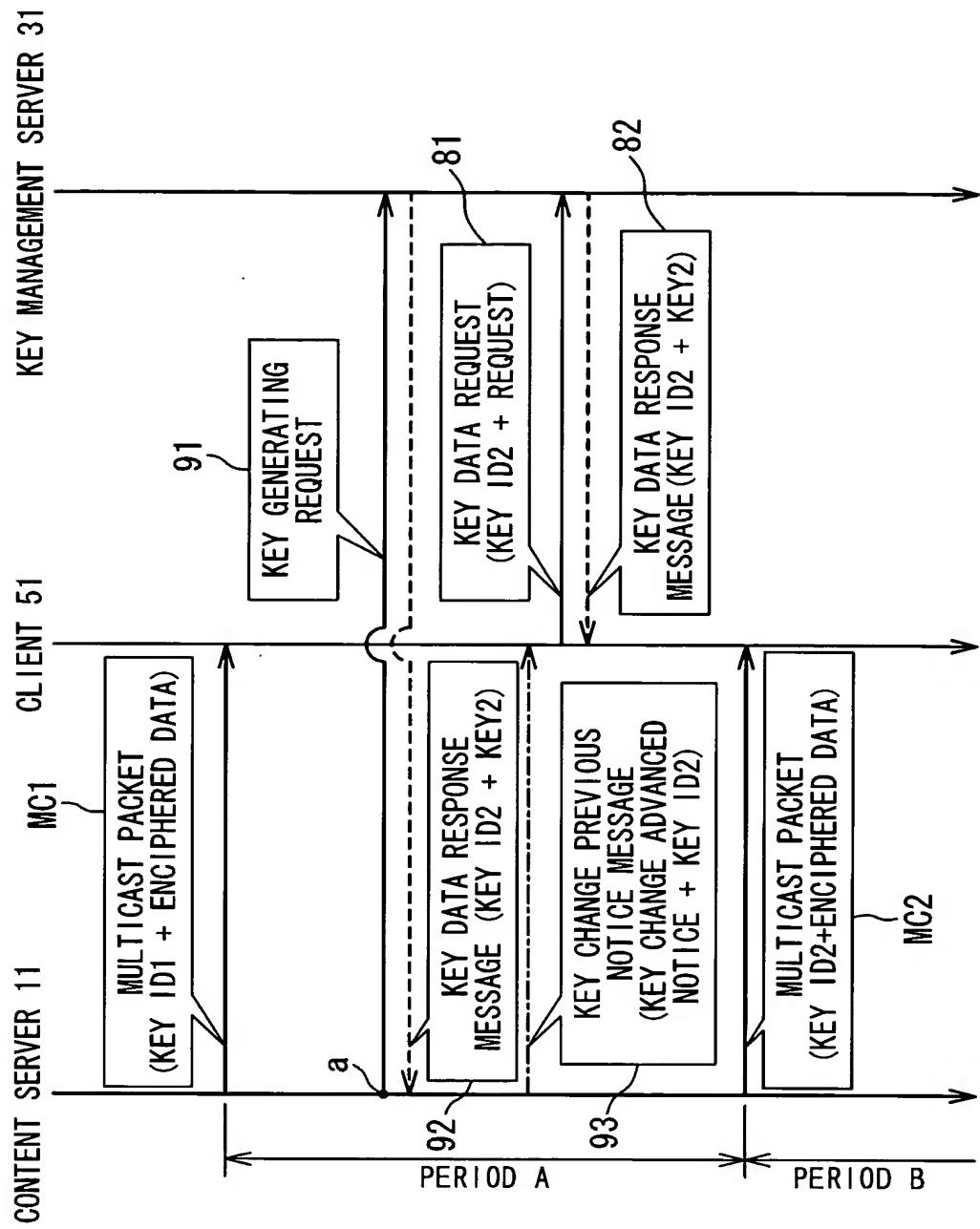


Fig. 19

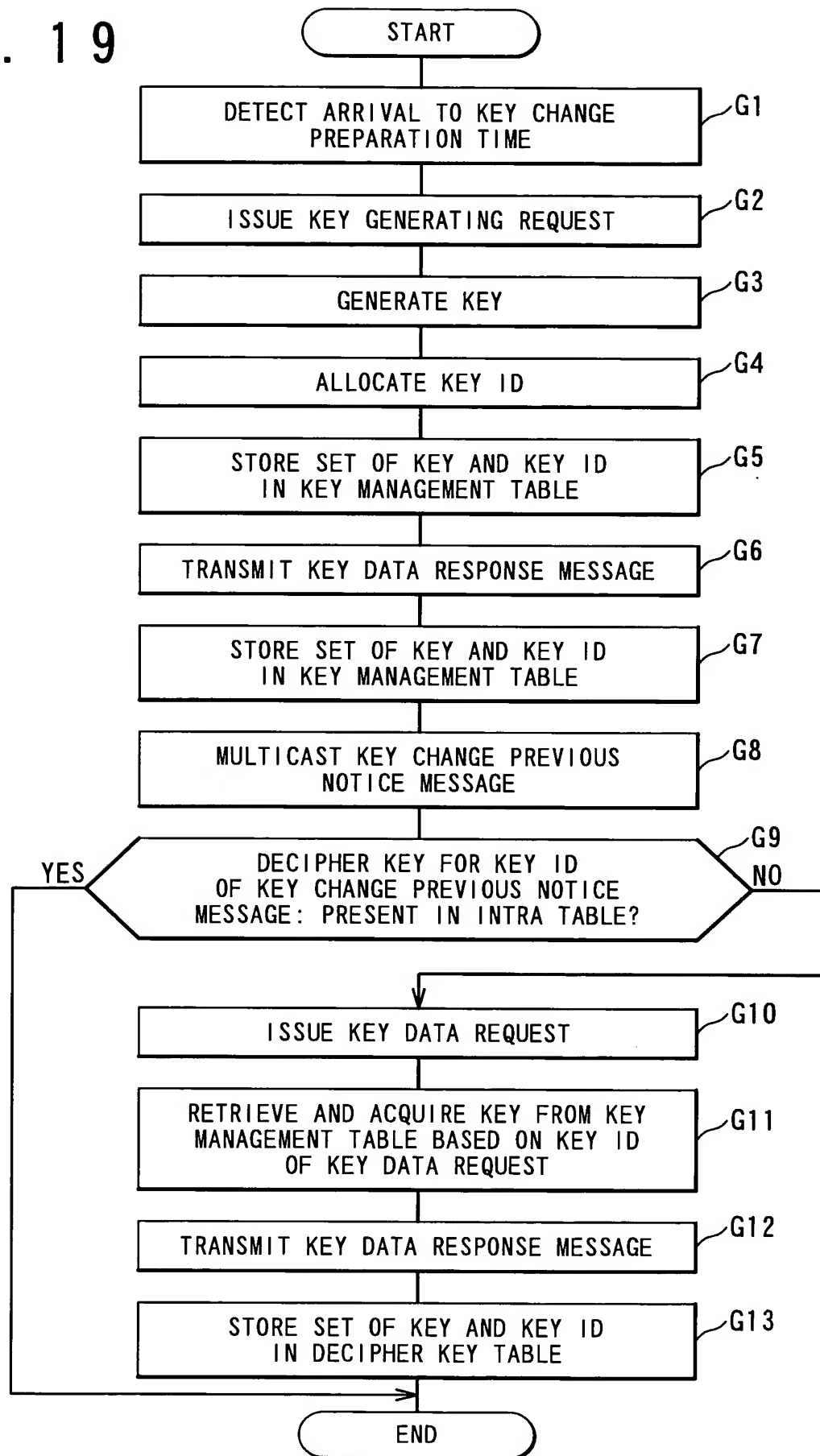
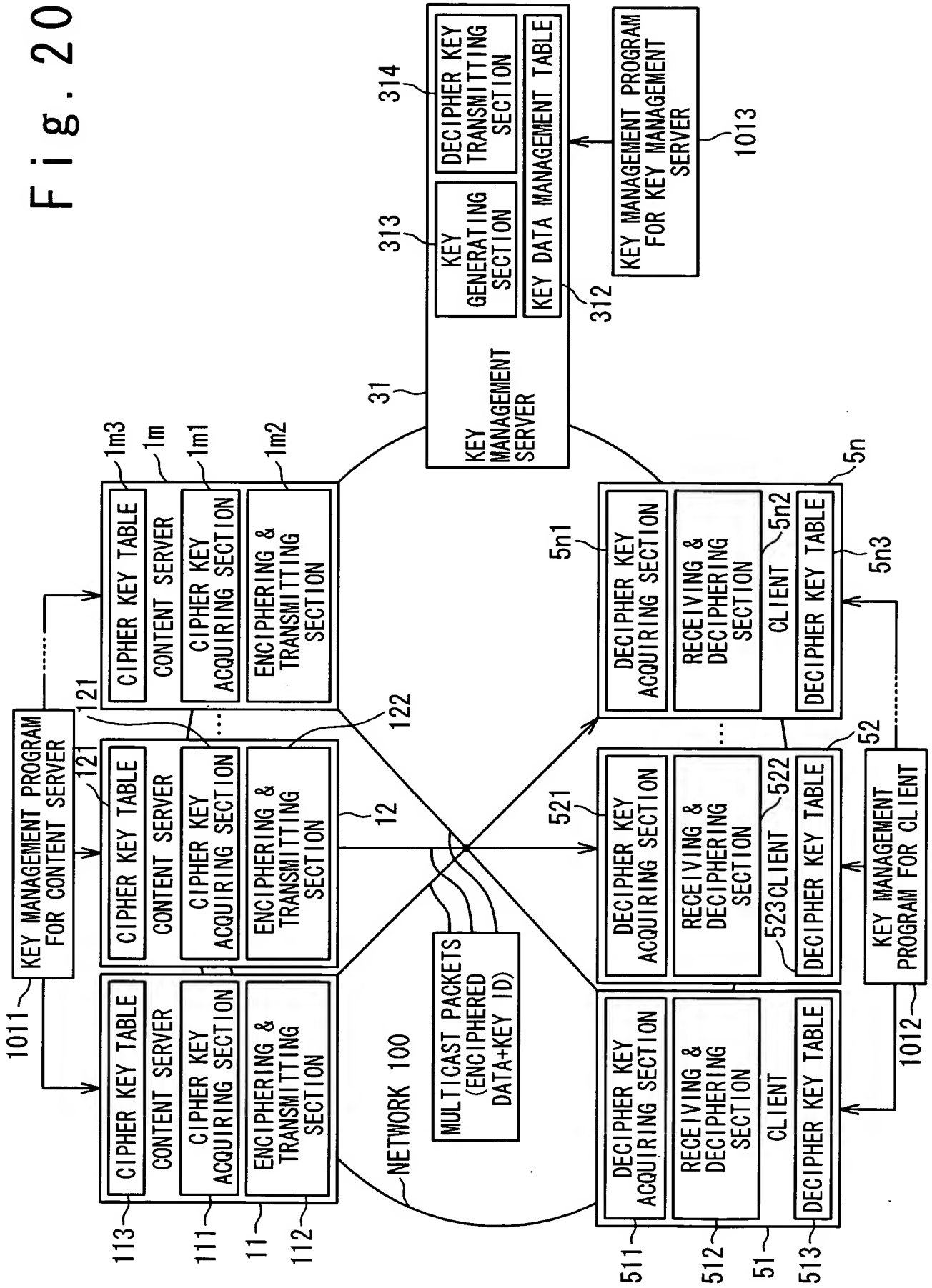


Fig. 20



# Fig. 21

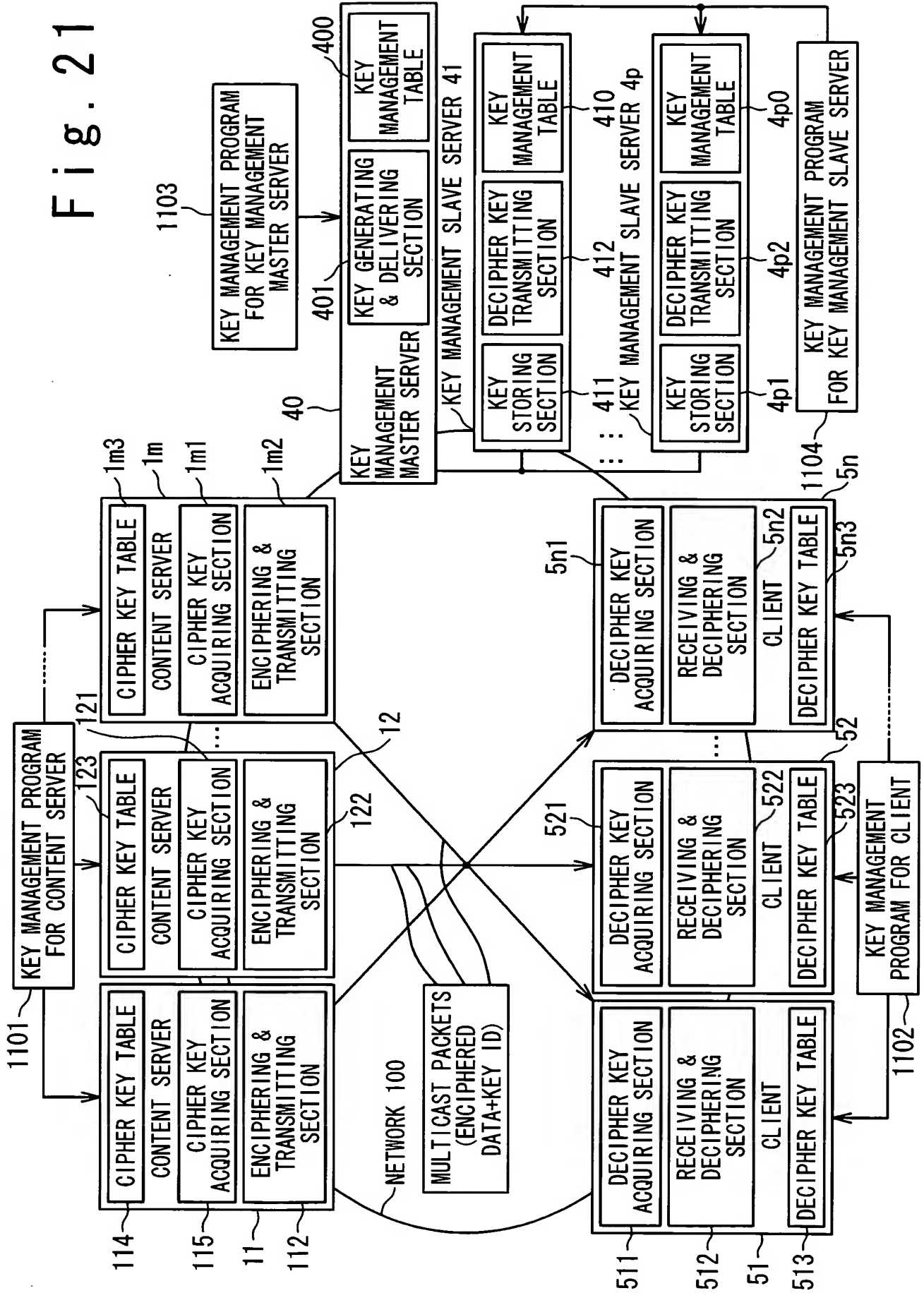


Fig. 22

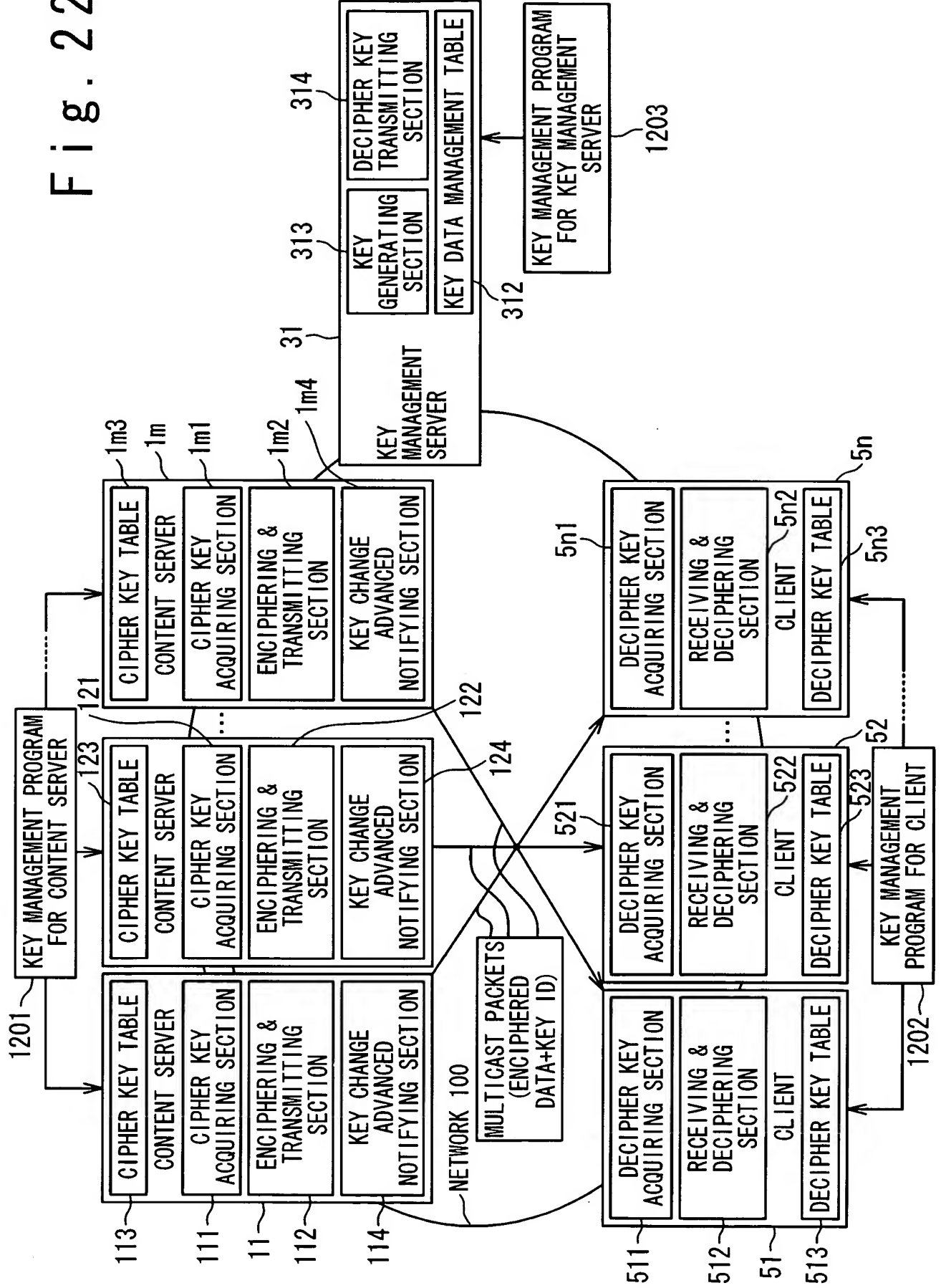


Fig. 23

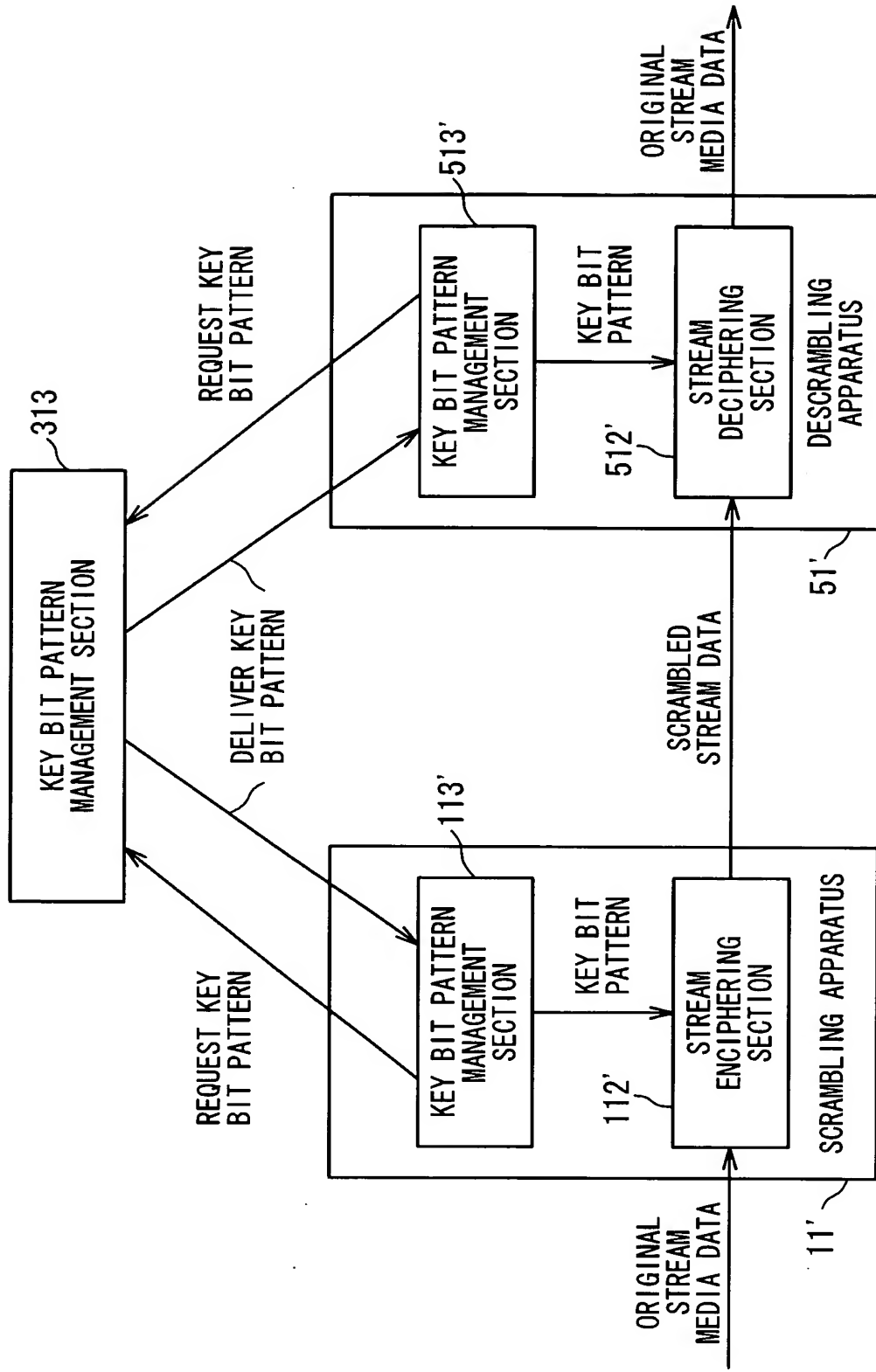
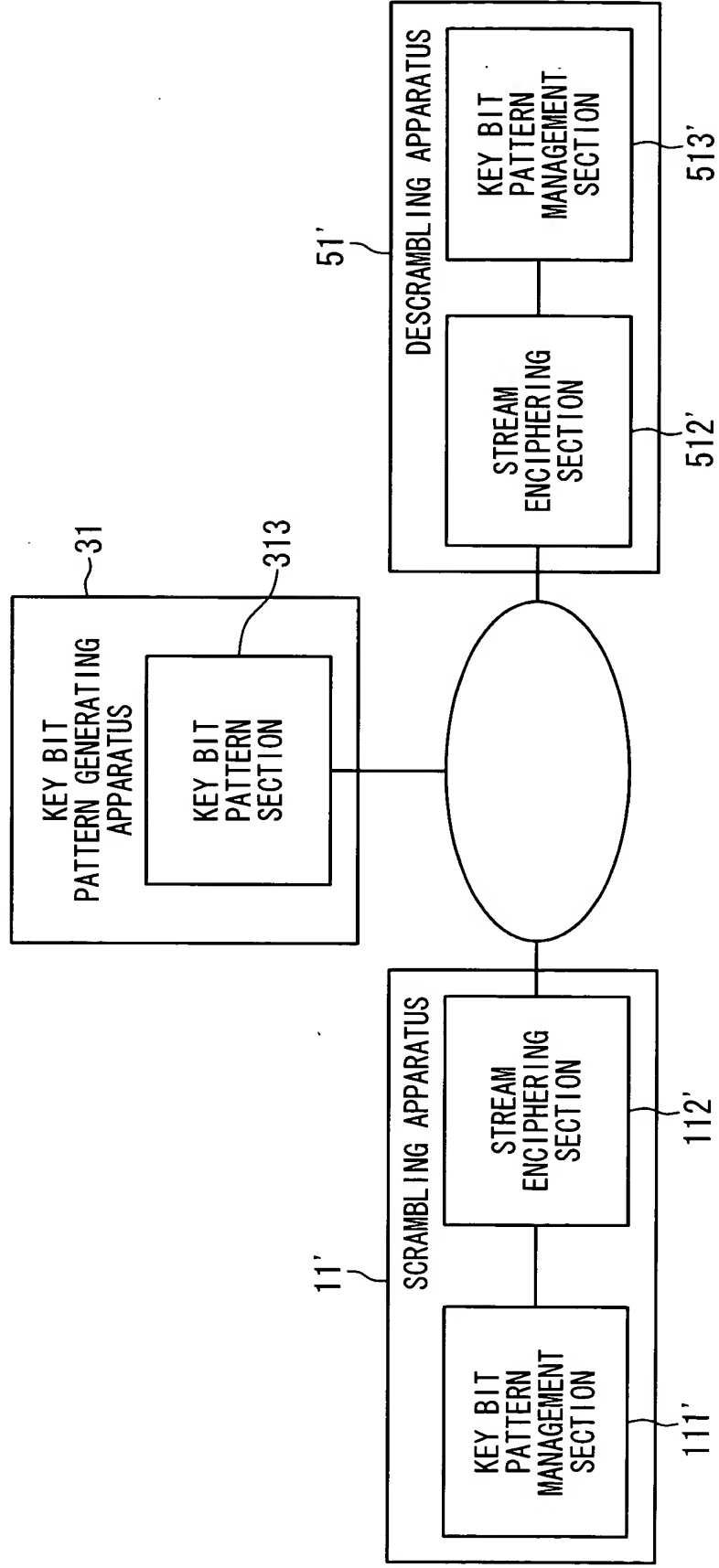
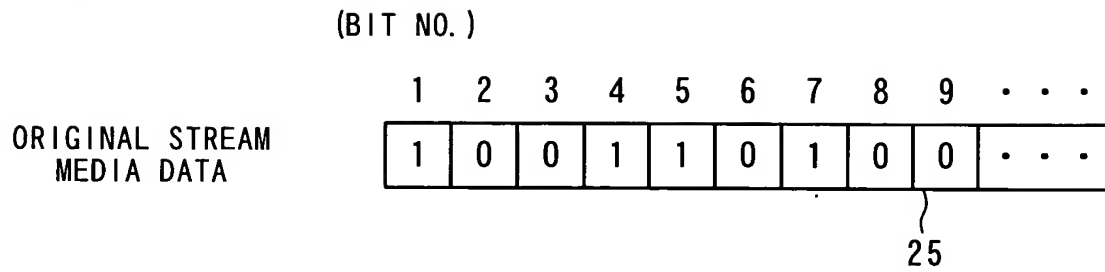


Fig. 24



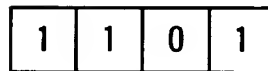


**F i g . 2 5 A**



**F i g . 2 5 B**

KEY BIT PATTERN



**F i g . 2 5 C**

SCRAMBLED STREAM DATA

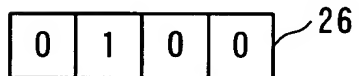


Fig. 26A

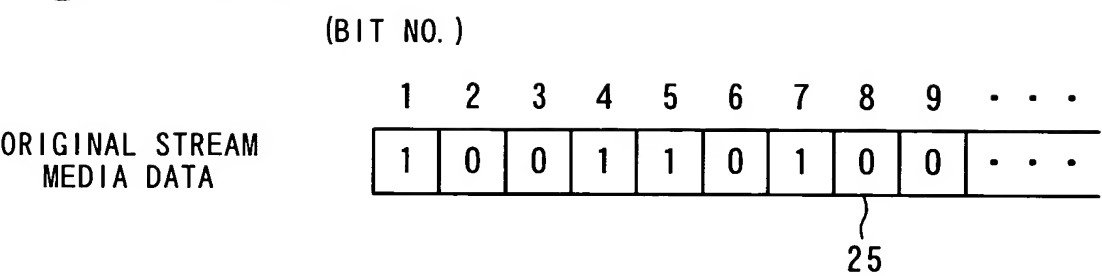


Fig. 26B



Fig. 26C

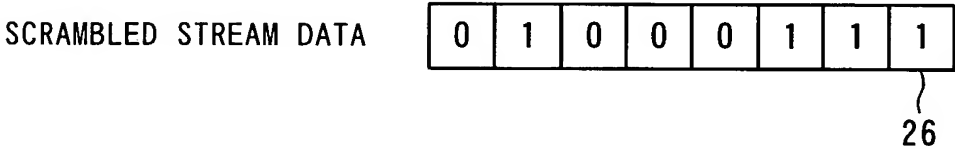


Fig. 27A

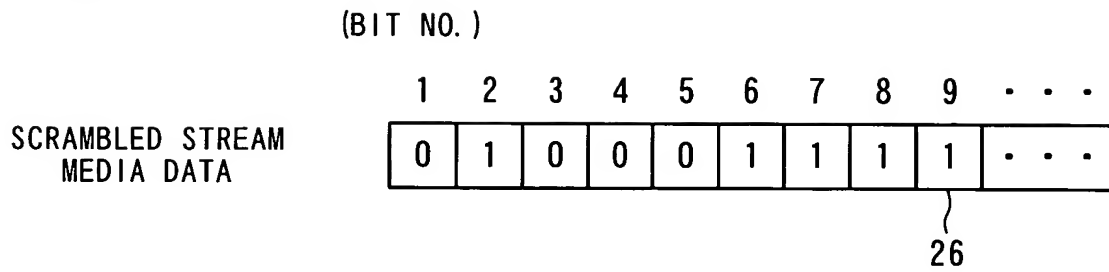


Fig. 27B

KEY BIT PATTERN

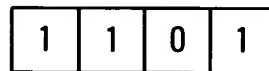
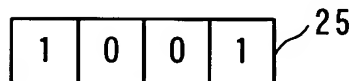
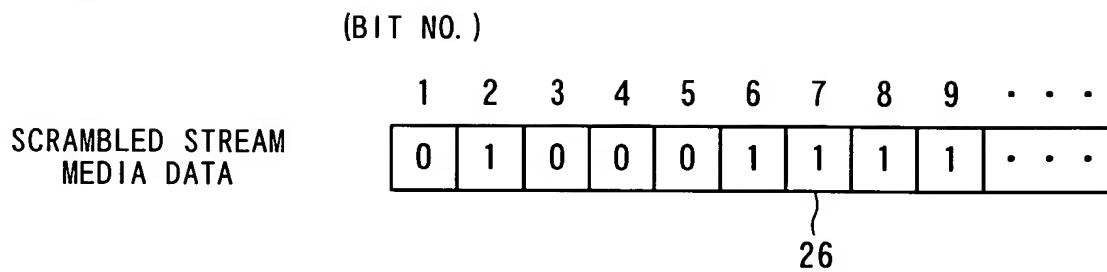


Fig. 27C

ORIGINAL STREAM DATA

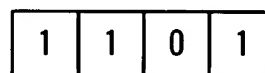


**F i g . 2 8 A**



**F i g . 2 8 B**

KEY BIT PATTERN



**F i g . 2 8 C**

ORIGINAL STREAM

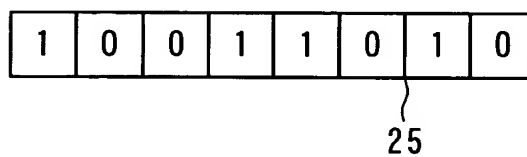


Fig. 29

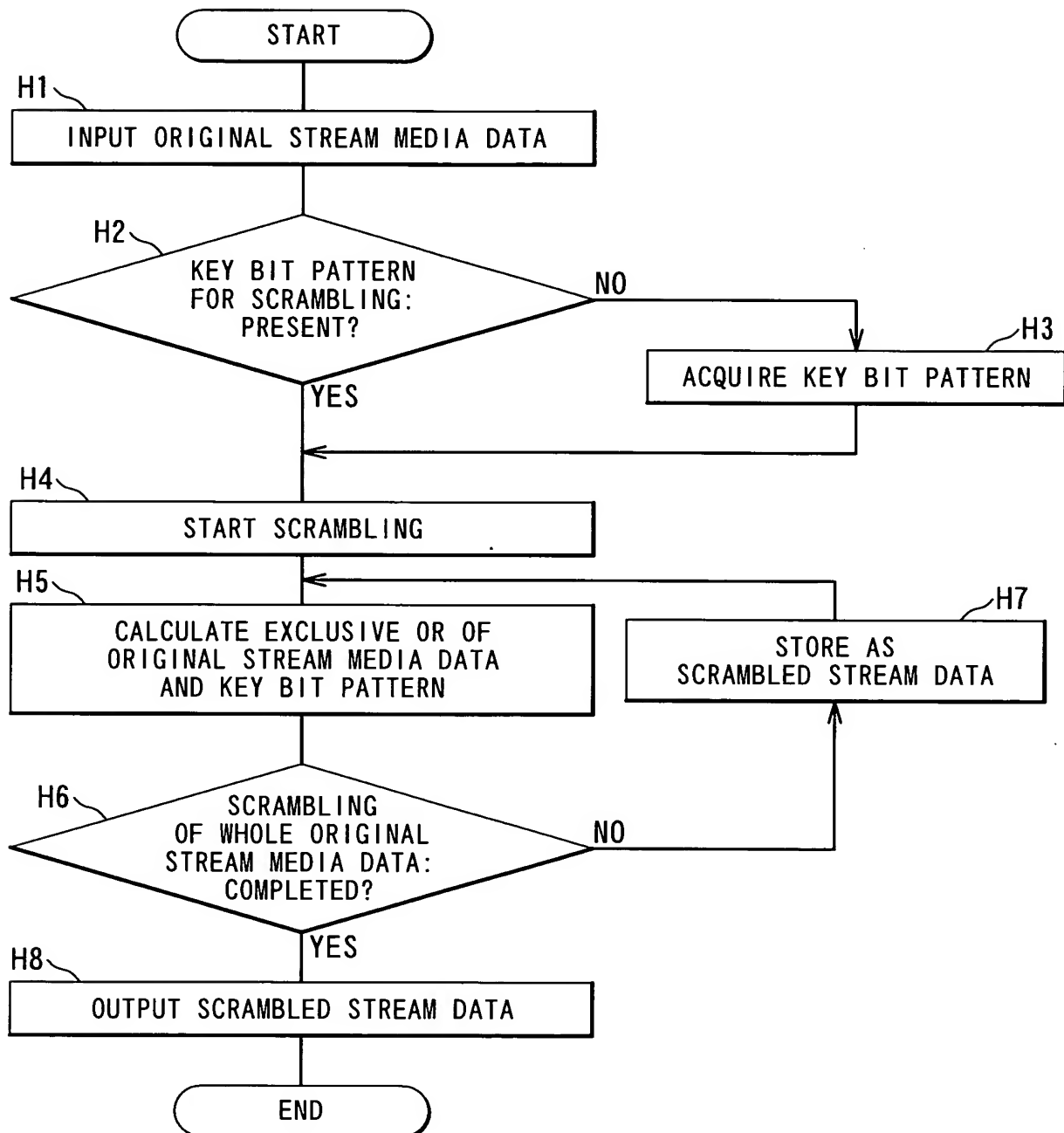


Fig. 30

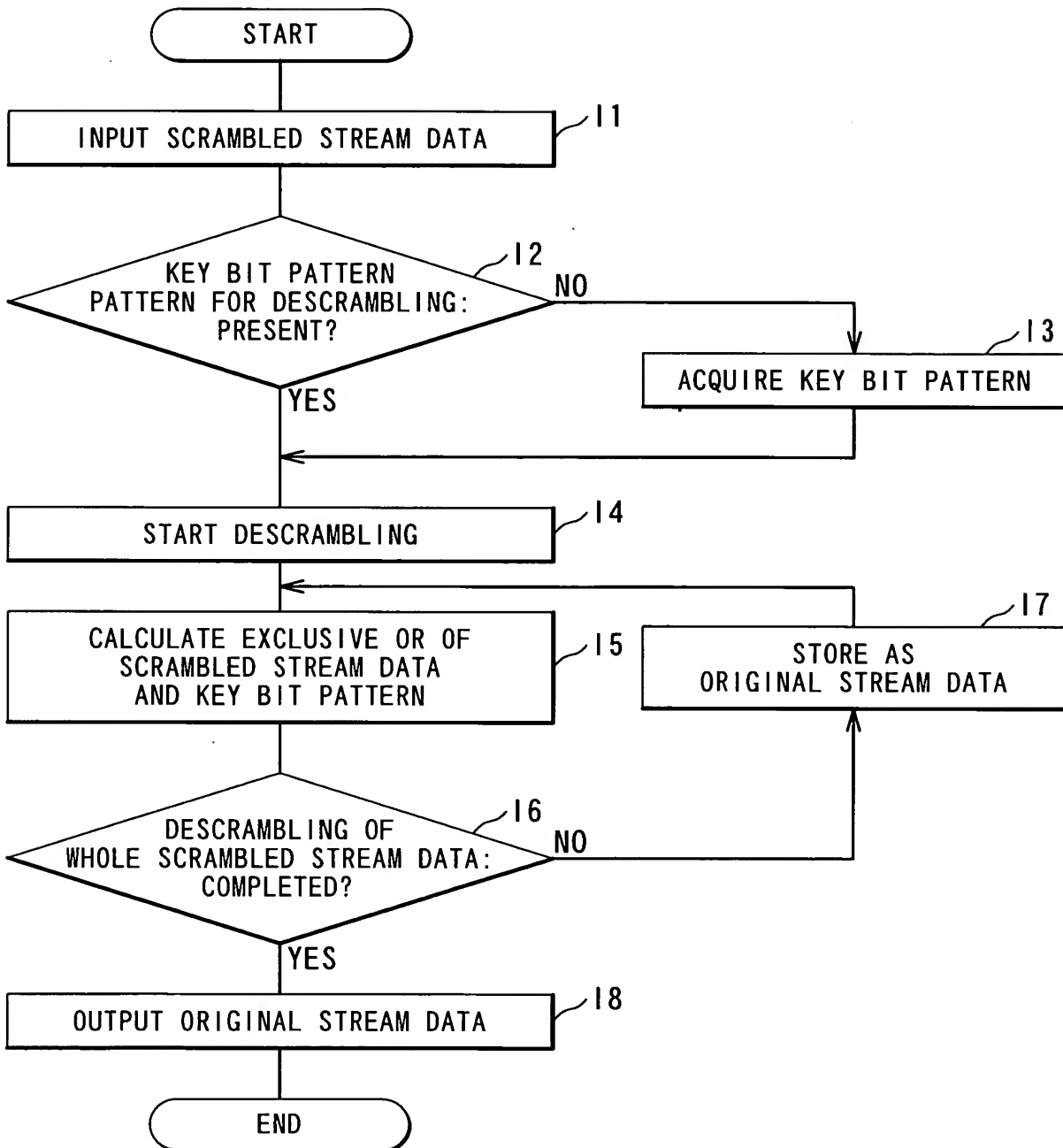


Fig. 31A

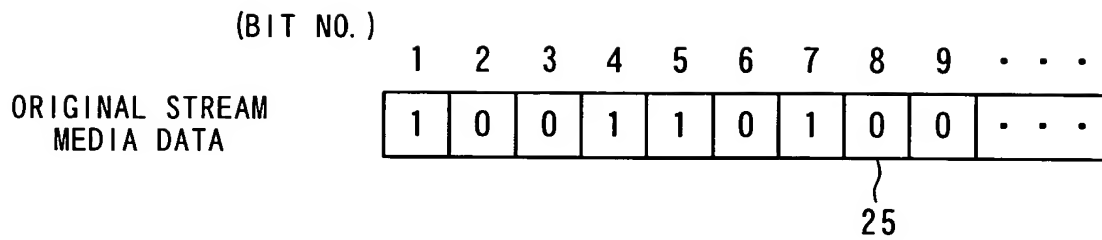


Fig. 31B



Fig. 31C



Fig. 31D

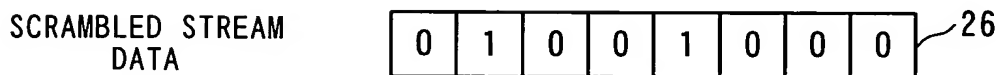


Fig. 32A

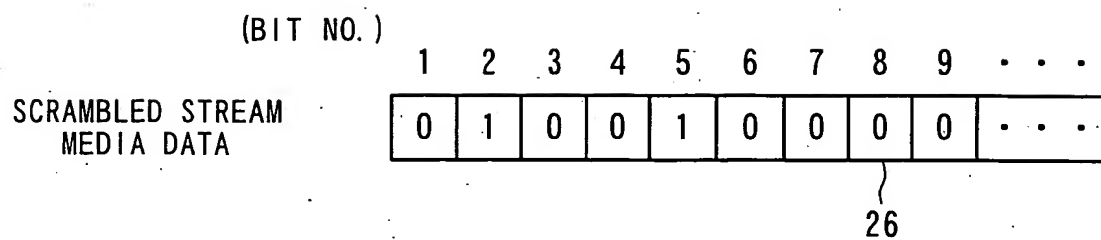


Fig. 32B

KEY BIT PATTERN

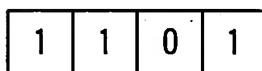


Fig. 32C

KEY BIT PATTERN

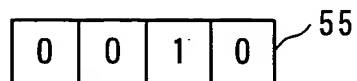


Fig. 32D

ORIGINAL STREAM  
DATA

